Crypto 01 (Snowden coordinates)

Snowden ha accedido a conceder dos entrevistas en dos ubicaciones diferentes, conocedor de que la CIA y el MI6 interceptan las comunicaciones ha decidido distribuir el riesgo de enviar a una sola persona las claves para desencriptar su ubicación y ha fraccionado la misma y la ha repartido entre varias personas, a priori 100. Obviamente solo la combinación de un número mucho más reducido de ellas permite reconstruir la clave para descifrar la localización. El sistema utilizado para el cifrado posee base polinómica para el cifrado/descifrado de la información.

Las coordenadas codificadas (valores X de entrada al polinomio) son: (40, 10), y (30, 20) y se sabe que Snowden está refugiado en Rusia, no está en el área asiática sino mas bien en una zona cercana al continente europeo. En relación a las coordenadas (40,10) proporcionan las coordenadas de la primera entrevista y las segundas (30,20) proporcionan las coordenadas de la segunda ubicación.

Los datos interceptados disponibles son los siguientes:

Valores X del polinomio:
34 18 76 19 87 22 25 20 20 20 35 19 77 6 54 63 91 24 68 70 47 46 77 25 34 6 86 95 10 98 9 12 39 38 36 3 79 35 1 47 4 89 58 9 46 73 89 20 75 86 49 49 64 0 99 29 5 52 18 76 16 93 61 63 2 37 85 31 96 55 26 11 21 71 86 67 39 7 48 68 2 32 53 43 90 86 98 16 28 30 73 33 64 45 15 59 43 16 4 86

Valores Y del polinomio:
58.21041 37.420200 58.009958 30.248782 29.759352 53.673387 51.722709 16.652384 33.619574 43.319465 50.890097 10.440974 46.366161 52.511702 8.093597 55.686039 47.857165 7.742006 52.693703 44.380174 39.892041 41.754565 54.513735 2.045807 36.830164 3.383975 2.998016 52.471324 11.511637 0.825278 6.098881 29.025281 8.828347 41.545796 49.325614 50.892328 33.239294 19.560255 8.244839 23.366817 0.431956 45.598040 9.373723 50.602918 16.142466 52.114783 39.467684 50.443156 53.684973 56.397021 16.546328 46.232761 44.911244 7.104355 37.250850 2.185266 19.171205 11.729428 38.991418 49.584929 19.253911 48.802050 42.217256 30.049673 59.649800 39.606704 46.869857 50.677991 10.988092 56.370226 11.934946 28.247432 47.648032 33.274334 18.405477 12.129523 44.501246 52.161999 34.811787 8.861618 32.973933 16.574644 4.117312 56.415139 44.871344 12.760921 42.446924 58.436670 43.650707 35.388661 10.973875 51.670235 7.523969 35.737060 3.403768 39.629694 53.848694 35.094827 53.50921 -867.6065

Los valores X e Y están asociados uno a uno, es decir, el primer punto x se corresponde con el primer punto y.

El formato de la solución debe ser el siguiente:
(coordenada1,coordenada2),(coordenada1,coordenada2)

Donde no hay espacios en blanco y el número de decimales para la primera coordenada (40,10) será de cuatro y seis para la segundas coordenadas (30,20).

Un ejemplo de solución es el siguiente, con flag{}:
(40.1234,10.1234),(30.123456,20.123456)

Crypto 01 – Solución

Se trata de un esquema de secreto compartido basado en polinomios lo que implica que la expresión general corresponde a un polinomio. En particular a un polinomio de grado tres, esto es:

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 x^0$$

La seguridad de este tipo de esquemas mediante polinomios se basa en el conocimiento de los coeficientes del mismo. Por tanto, es necesario conocer al menos (en este caso que es de grado 3) cuatro puntos (x,y) y resolver los sistemas de ecuaciones.

Siguiendo el enunciado, en realidad hay muchos puntos (x,y) lo que quiere decir que debemos comprobar combinaciones de n elementos tomados de cuatro en cuatro. Dado que se pueden generar muchas soluciones la forma de verificar la validez es mediante la pista proporcionada, que es la localización en un área geográfica muy extensa.

Como resultado los valores necesarios para iniciar la resolución del sistema de ecuaciones es la siguiente, se marca en negrita para mejorar su identificación.

Valores X del polinomio:

34 18 76 19 87 22 25 20 20 20 35 19 77 6 54 63 91 24 68 70 47 46 77 25 34 6 86 95 10
98 9 12 39 38 36 3 79 35 1 47 4 89 58 9 46 73 89 20 75 86 49 49 64 0 99 29 5 52
18 76 16 93 61 63 2 37 85 31 96 55 26 11 21 71 86 67 39 7 48 68 2 32 53 43 90 86 98 16
28 30 73 33 64 45 15 59 43 16 **4 86**

Valores Y del polinomio:

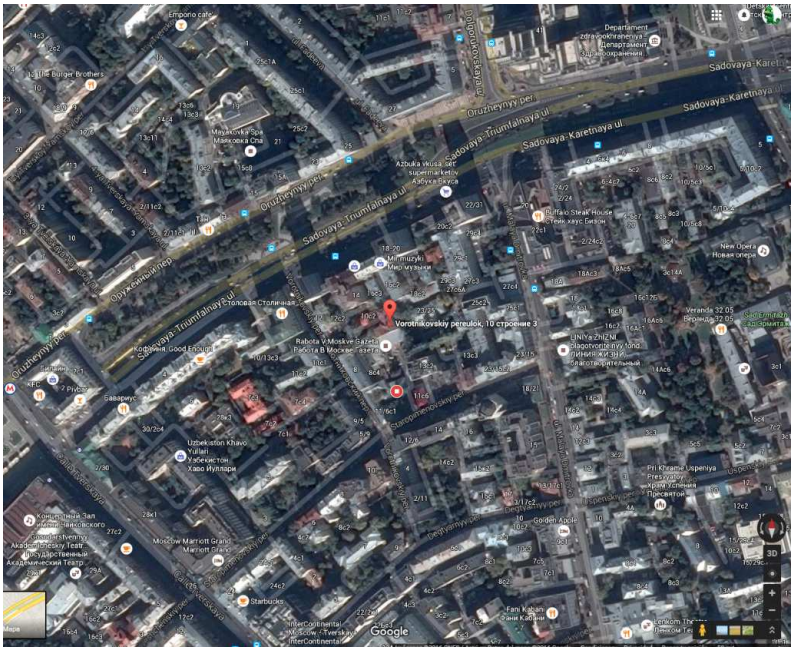
58.21041 37.420200 58.009958 30.248782 29.759352 53.673387 51.722709 16.652384
33.619574 43.319465 50.890097 10.440974 46.366161 52.511702 8.093597 55.686039
47.857165 7.742006 52.693703 44.380174 39.892041 41.754565 54.513735 2.045807
36.830164 3.383975 2.998016 52.471324 11.511637 0.825278 6.098881 29.025281
8.828347 41.545796 49.325614 50.892328 33.239294 19.560255 8.244839 23.366817
0.431956 45.598040 9.373723 50.602918 16.142466 52.114783 39.467684 50.443156
53.684973 56.397021 16.546328 46.232761 44.911244 7.104355 37.250850 2.185266
19.171205 11.729428 38.991418 49.584929 19.253911 48.802050 42.217256 30.049673
59.649800 39.606704 46.869857 50.677991 10.988092 56.370226 11.934946 28.247432
47.648032 33.274334 18.405477 12.129523 44.501246 52.161999 34.811787 8.861618
32.973933 16.574644 4.117312 56.415139 44.871344 12.760921 42.446924 58.436670
43.650707 35.388661 10.973875 51.670235 7.523969 35.737060 3.403768 39.629694
53.848694 35.094827 **53.50921 -867.6065**

A partir de estos valores se obtienen los coeficientes del siguiente polinomio:

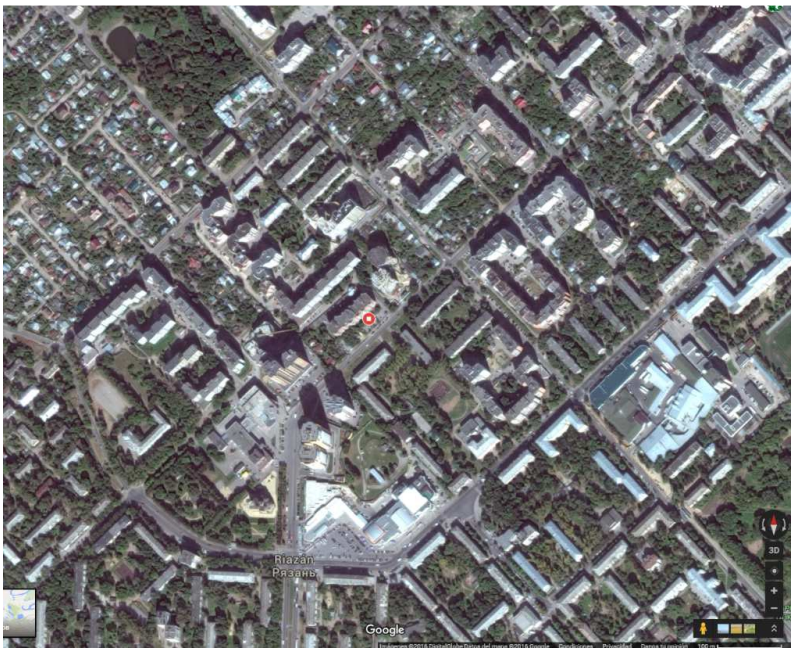
y=-0.0044214*x*x*x+0.3292185*x*x-6.570405*x+74.8063

En el enunciado se indica que se proporcionan las coordenadas de las reuniones, que son los valores X de entrada al polinomio. El resultado de estas coordenadas es el siguiente:

Coordenada 1: (40,10) que se traduce en las coordenadas 55.7701 37.6027 que se corresponden a un barrio de Moscú.



Coordenada 2: (30,20) que se traduce en las coordenadas 54.646837, 39.714275 que se corresponden a una ciudad rusa Sovetskiy rayon.



Crypto 02 (Quantum)

La NSA ha iniciado el proceso de diseño de algoritmos de encriptación robustos a la computación cuántica. Mientras tanto ha empezado a utilizar los primeros resultados en este campo para la distribución de claves simétricas, en particular el protocolo criptográfico cuántico llamado BB84.

Dada lo novedoso del asunto, se ha puesto en marcha el sistema de distribución de claves solo entre dos oficinas de la NSA, una ubicada en New York y la otra en Munich.

El sistema a diferencia de los planteamientos originales se ha basado en un sistema cuántico de 3 niveles en lugar de dos, evitando el uso de las bases cuánticas más utilizadas y por tanto robusteciendo el sistema. En base a este sistema cuántico se han empezado a transmitir los primeros bloques de información, que consisten en el envío de índices numéricos en libros de códigos criptográficos.

Pero se ha producido una fuga de información y se ha obtenido la configuración de los estados cuánticos que permite deducir las probabilidades de los mismos (véase fichero adjunto):

$$|\psi\rangle = \left(\frac{1}{2} + \frac{i}{2}\right)|0\rangle + \left(-\frac{1}{2}\right)|1\rangle + \left(\frac{i}{2}\right)|2\rangle$$

Y además se conocen las siguientes transmisiones de bloques de información:

1111 0100 1010 0020
1010 1010 1110 1100
0101 1000 1101 0100
1011 0101 0100 1201
1111 0100 1010 0020
1010 1010 1110 1100
0101 1000 1101 0100
1011 0101 0100 1201
1111 0100 1010 0020
1010 1010 1110 1100
0101 1000 1101 0100
1011 0101 0100 1201
1111 0100 1010 0020
1010 1010 1110 1100
0101 1000 1101 0100
1011 0101 0100 1201

¿Cual es la posición de las bases para poder descifrar el resto de los mensajes?

Cada posición se debe indicar con el número de la base: 0, 1 o 2, y si no hay detector un guión "-". Pudiendo ser una posible solución la siguiente: flag{0001-11--22110120}

Nota 1: No se produce la clásica pérdida del 50% de la información.

Nota 2: Las estadísticas TIENEN que ser exactas para poder seleccionar un detector, es decir, si dos valores estadísticos uno corresponde de forma exacta a la probabilidad de una de las bases y otra no, se aceptará como buena la primera.

Nota 3: Si ninguna estadística calculada se corresponde de forma exacta con ningún valor de probabilidad, se dará por inválida la lectura del bit, y no se considerará como válida la ubicación de un detector.

Crypto 02 – Solución

El enunciado señala que se ha puesto en marcha el protocolo de intercambio de claves cuántico llamado BB84.

El protocolo es perfecto, pero se indica que la NSA lo ha complicado. Y esta complicación provoca una complejidad elevada y es utilizar un sistema de k niveles cuánticos en particular 3 niveles. El hecho de utilizar tres niveles provoca que aún utilizando los detectores adecuados la probabilidad de obtener el valor correcto NO sea uno, sino un valor inferior a uno, en particular las probabilidades que se obtienen de los coeficientes son:

P(0)=1/2

P(1)=1/4

P(2)=1/4

Esto provoca que obligatoriamente sea necesario emitir múltiples tramas, calcular las estadísticas y determinar el valor que mejor ajusta a las probabilidades esperadas.

Esta es la dificultad real del problema, en este caso se proporcionan las probabilidades de los tres estados cuánticos y además se proporcionan un conjunto de tramas de bits, es decir, información suficiente para calcular las estadísticas y determinar el valor que más se ajusta a las probabilidades proporcionadas.

Realizando este cálculo por columnas (aunque solamente es necesario utilizar las primeras cuatro líneas ya que se repiten) obtenemos lo siguiente:

Bloque 1-4

Bit 0: P(0)=1/4, P(1)=3/4. Detector inválido.
Bit 1: P(0)=1/2, P(1)=1/2. El detector debe estar en el estado “0”.
Bit 2: P(0)=1/4, P(1)=3/4. Detector inválido.
Bit 3: P(0)=1/4, P(1)=3/4. Detector inválido.

Bit 5: P(0)=1/2, P(1)=1/2. El detector debe estar en el estado “0”.
Bit 6: P(0)=1/2, P(1)=1/2. El detector debe estar en el estado “0”.
Bit 7: P(0)=1/4, P(1)=3/4. El detector debe estar en el estado “1”.
Bit 8: P(0)=3/4, P(1)=1/4. El detector debe estar en el estado “1”.

Bit 9: P(0)=1/4, P(1)=3/4. Detector inválido.
Bit 10: P(0)=1/2, P(1)=1/2. El detector debe estar en el estado “0”.
Bit 11: P(0)=1/2, P(1)=1/2. El detector debe estar en el estado “0”.
Bit 12: P(0)=3/4, P(1)=1/4. El detector debe estar en el estado “1”.

Bit 13: P(0)=1/42 P(1)=1/2. El detector debe estar en el estado “0”.
Bit 14: P(0)=1/4, P(1)=1/2, P(2)=1/4. El detector debe estar en el estado “2”.
Bit 15: P(0)=3/4, P(2)=1/4. El detector debe estar en el estado “2”.
Bit 16: P(0)=3/4, P(1)=1/4. El detector debe estar en el estado “1”.

Solución/Posición de los detectores: `-0--0011-0010221`